Evaluation of the role of access providers. Discussion of Dutch Pirate Bay case law and introducing principles on directness, effectiveness, costs, relevance, and time

Lodder, A.R.; van der Meulen, N.S.

published in
Journal of Intellectual Property, Information Technology and E-Commerce Law
2013

EVALUATION OF THE ROLE OF ACCESS PROVIDERS

DISCUSSION OF DUTCH PIRATE BAY CASE LAW AND INTRODUCING PRINCIPLES ON DIRECTNESS, EFFECTIVENESS, COSTS, RELEVANCE, AND TIME

Arno R. Lodder[1] & Nicole S. van der Meulen[2]
VU University Amsterdam, Department Transnational Legal Studies
Center for Law and Internet
Amsterdam, The Netherlands

Abstract

Internet Service Providers (ISPs) play a pivotal role in contemporary society as they provide access to the internet. The primary task of ISPs, to blindly transfer information across the network, has recently come under pressure, as has their status as neutral third parties. Both the public and the private sector have started to require ISPs to interfere with the content placed and transferred on the Internet as well as access to it, for a variety of purposes including the fight against cybercrime, digital piracy, child pornography, etc. This expanding list asks for a critical assessment of the role of ISPs. This paper analyses the role of the access provider. Particular attention is paid to Dutch case law in which access providers were forced to block the Pirate Bay. After analyzing the position of ISPs, we define principles that can guide the decision of ISPs to take action or not after a request to block access based on directness, effectiveness, costs, relevance, and time.

A. Introduction

Traditionally, third parties facilitating communication and information exchange were mere messengers or neutral transporters. As a popular Dutch saying goes,[3] their policy should be to not take notice of the content of messages. Postal services do not open letters, telephone companies do not eavesdrop on communication, even classic operators just made the connection. Only to some services knowledge of the content is inherent, like in case of telegrams and telex.

In the early days of the internet, ISPs still fitted into the tradition of communication neutrals. From the moment internet access has been provided to the general public, early 1990s, crime slowly started to take off and in particular copyright infringements increased quite exponentially. These developments led to a changing role of Internet Service Providers. No longer could they maintain a completely neutral position.

[1] Professor of Internet Governance and Regulation at VU University Amsterdam.
[2] Assistant Professor of Internet Governance at VU University Amsterdam.
[3] The Dutch phrase is often used to emphasize the neutral position of Internet Service Providers and has a difficult to translate repetition of words: “geen boodschap aan de boodschap”.

The initial attempts to regulate ISPs, with as most prominent examples the US Digital Millennium Copyright Act (DMCA)[4] and the European Union Directive 2000/31/EC on electronic commerce (Directive on e-commerce),[5] reflected a new dual role of internet intermediaries: they deserved protection as neutrals, but could also be called upon to assist with norm enforcement. The underlying reason for these regulations, however, primarily was to define exceptions or safe harbors that would protect ISPs against liability claims. Nevertheless, these laws also acknowledged that ISPs under certain circumstances should assist in stopping, e.g., copyright infringements.

Both the DMCA and the Directive on e-commerce[6] regulated three types of ISP services, viz. the transport, temporary storage, and hosting of information. In addition, the DMCA also regulated search engines. Presently, there is a tendency to put pressure on ISPs to co-operate in addressing norm violation, in particular in their role as access provider. For instance, courts in several countries (Netherlands, Finland,[7] UK,[8] etc.) ordered ISPs to filter internet traffic, the French HADOPI Act has a so-called three strike policy regarding downloading, and the controversial ACTA is impeding on human rights in a serious way.[9] The secrecy surrounding this latter initiative added to the controversy regarding its content. Many media attention was also paid to the US initiatives SOPA and PIPA.[10] These initiatives were abandoned in February 2012, but already in April 2012 the comparable CISPA passed the House of Representatives.[11] Since the Senate did not accept the CISPA, it was re-entered and passed again in April 2013.[12]

Are the time's changing, are we entering a new era? This paper aims to answer this question, and focuses the discussion on ISPs in their role as access provider.[13] The paper is structured as follows. In section 2 the liability exemptions of the US DMCA and the EU Directive on e-commerce are introduced. Next, we discuss a series of Dutch court cases concerning The Pirate Bay that ended in 2012 with court orders against several ISPs to, basically, filter out websites that belong to the Pirate Bay. In the third part we evaluate which role fits access providers best. From different angles the access provider as the

[4] 112 STAT. 2860 PUBLIC LAW 105–304—OCT. 28, 1998, 105th Congress. An Act to amend title 17, United States Code, to implement the World Intellectual Property Organization Copyright Treaty and Performances and Phonograms Treaty, and for other purposes. The present paper covers one of the "other purposes", limitations on liability for ISPs.

[5] Directive 2000/31/EC on electronic commerce, see above, footnote **Error! Bookmark not defined.**.

[6] For an extensive overview of case law ruled under both initiatives see M. Martinet Farano (2012), *Internet Intermediaries' Liability for Copyright and Trademark Infringement: Reconciling the EU and U.S. Approaches*, TTLF Working Papers No. 14.

[7] M. Norrgård (2011), Blocking Web Sites – Experiences from Finland, http://ssrn.com/abstract=1997103.

[8] The High Court of England and Wales ruled on April 30 2012 after claims from the British Phonographic Industry (BPI) that five ISPs (Sky, Everything Everywhere, TalkTalk, O2 and Virgin Media) should block the Pirate Bay, see e.g. *Huffington Post* 30 April 2012, http://huff.to/OGhD5m

[9] P.K. Yu (2011), Six Secret (and Now Open) Fears of ACTA. *SMU Law Review, Vol. 64,* pp. 975-1094, 2011.

[10] M.A. Carrier (2012), Copyright and Innovation: The Untold Story. *Wisconsin Law Review*, Forthcoming. Available at SSRN: http://ssrn.com/abstract=2099876

[11] Cyber Intelligence Sharing and Protection Act, Passed the US House of Representatives on April 26. 2012. See http://thomas.loc.gov/cgi-bin/query/z?c112:H.R.3523:. It is uncertain whether the US Senate accepts the bill, and if it does, President Obama has indicated not to sign.

[12] H.R. 624: Cyber Intelligence Sharing and Protection Act, accepted on April 18 2013, http://www.govtrack.us/congress/votes/113-2013/h117.

[13] The access provider was not explicitly mentioned in the two main 1990s regulations, but is commonly headed under mere conduit (EU Directive) or transitory communications (DMCA), see further below the section *Early days: DMCA and Directive on e-commerce*.

intermediary merely providing access to the internet is weighed against the access provider as a full time norm enforcer, and we provide principles that can help in striking a balance.

B. Early days: DMCA and Directive on e-commerce

The spirit of the mid 1990s is well reflected by Kaspersen:[14]

" (…) the duties of access-providers do not embody anything else but giving access to the Net and all the information in it, just as it is."

Stated simply, an access provider should just provide access to the internet. This basically was the background of the legislation proposed during the late 1990s, although besides this main focus on creating a safe harbor it was also acknowledged that under certain circumstances ISPs should assist in combating (in particular copyright) infringements.

I. DMCA

Prior to the DMCA in 1996 Section 230 of the Communications Decency Act regulated immunity for, e.g. ISPs, regarding hosted content.[15] For the present paper with its focus on access providers this controversial and much debated Act[16] is not directly relevant.

On December 1998 the DMCA entered into force. This Act included in Title II the addition of paragraph 512 to the US Code, better known as the *Online Copyright Infringement Liability Limitation Act (OCILLA)*. OCILLA defines four categories of exemptions applicable to ISPs, viz. regarding services related to (1) information location tools (search engines), (2) storage of information at direction of users (hosting), (3) system caching, and (4) transitory communications.[17] The transitory communications are relevant for the present paper since it concerns "transmitting, routing, or providing connections." Whereas in doctrine, access providers are normally distinguished as a special category of providers, in regulation this is not necessarily the case. Although all types of transitory communication providers are crucial to a proper functioning of the internet, the doctrinal treatment of access providers as a single category is understandable. For anyone on the internet, it always starts with getting access.

Instead of enforcing norms on the internet, regulating behavior *in* cyberspace, it is sometimes easier to control at the source: make sure that people never get to (parts) of the internet, or that people cannot use particular applications. As such the ISP can function as a single point of contact for all of its users, and these users are regulated at a single instance.

[14] H.W.K. Kaspersen, Liability of Providers of the Electronic Highway, 12 *The Computer Law and Security Report* 2006: 290-293.

[15] M. Schruers (2002), The History and Economics of ISP Liability for Third Party Content, *Virginia Law Review*, Volume 88, No. 1, pp 205-64.

[16] D.S. Ardia (2010), Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity Under Section 230 of the Communications Decency Act. *Loyola of Los Angeles Law Review*, Vol. 43, No. 2, 2010.

[17] Reese nicely characterizes the nature of the exemptions: "Congress has enacted, in section 512 of the Copyright Act, limitations on the liability of service providers, but conditioned those limitations on a fairly complicated set of conditions." R.A. Reese, The Relationship between the ISP Safe Harbors and Liability for Inducement. *Stanford Technology Law Review*, Vol. 8, 2011.

Access providers are the gate to the virtual world, and consequently are an obvious party to appoint as norm enforcer, viz. gate keeper. As Mann & Belzey state:[18]

"Internet intermediaries (…) are easy to identify and have permanent commercial roots inside the jurisdictions that seek to regulate the internet."

As a shelter for such claims, the DMCA/OCILLA determines that the transitory communication provider is not liable if (1) he does not initiate the access, (2) the process is automatic without selection of the material, (3) he does not determine recipients, and (4) the information is not modified. Besides these topics related to the core activity of an ISP, the OCILLA sets two other conditions, viz. (5) providers should have a policy of account termination of repeat infringers, and (6) should not interfere with technical measures (e.g., Digital Rights Management software).

Access providers almost intrinsically satisfy all these conditions expect for the fifth. Basically, in a normal course of action, access providers cannot be held liable as long as they define and apply a policy of account termination. The above applies to monetary relief. There are some circumstances under which injunctive or other equitable relief is possible,[19] and we discuss them after introducing the E-commerce directive.

II. Directive 2000/31/EC on e-commerce

The e-commerce directive was drafted against another background than the DMCA. The opening words of the proposal for the e-commerce directive are illustrative:

"Electronic commerce offers the Community a unique opportunity for economic growth, to improve European industry's competitiveness and to stimulate investment in innovation and the creation of new jobs."[20]

This Directive formed the central pillar in the regulation of e-commerce within the EU, as was outlined in a policy document from 1997.[21] As part of the same legal package the Directive 2001/29/EC on copyright in the information society is more directly related to the DMCA, but it did not cover liability:[22]

[18] R. J. Mann and S.R. Belzley, The Promise of Internet Intermediary Liability. *William and Mary Law Review*, Vol. 47, October 2005.

[19] As defined in § 512 subsection (j).

[20] Proposal for a EUROPEAN PARLIAMENT AND COUNCIL DIRECTIVE on certain legal aspects of electronic commerce in the internal market, 18.11.1998, COM(1998) 586 final, p. 3.

[21] "A European Initiative on Electronic Commerce", COM(97) 157 final, 16.4.1997.

[22] Recital 16 DIRECTIVE 2001/29/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, *OJ*, 22.6.2001, L 167/10. The proposal for this Directive was published 10 December 1997, almost a year before the e-commerce directive: 18 November 1998. The final text, however, was published one year later (June 2000 and June 2001 respectively). The member states had far more problems agreeing on how to regulate copyright on the internet, than they had to agree on how to regulate e-commerce. For a discussion of this Directive see M. Vivant (2002), Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, in Lodder, A.R., Kaspersen, H.W.K. (eds.), *eDirectives: Guide to European Union Law on E-Commerce* , Kluwer Law International, The Hague, p. 95-117.

"Liability for activities in the network environment concerns not only copyright and related rights but also other areas, such as defamation, misleading advertising, or infringement of trademarks, and is addressed horizontally in Directive 2000/31/EC (…) on e-commerce"

In the proposal for the e-commerce directive the European Commission identified five key issues, referred to as obstacles. One of them concerned the liability of intermediaries:

"To facilitate the flow of electronic commerce activities, there is a recognised need to clarify the responsibility of on-line service providers for transmitting and storing third party information (i.e. when service providers act as "intermediaries")."[23]

The angle is basically economic. The aim is to stimulate e-commerce within the European Union by protecting ISPs against liability, so preventing they would be hindered by all kind of liability claims when providing their services. Nonetheless, the Directive on e-commerce[24] takes a similar approach, and as McEvedy correctly observes[25] "closely resembles the DMCA in that it provides 'limitations of liability' while leaving the underlying law unaffected". The scope of the e-commerce directive is broader, in that it covers all legal fields, not only copyright. Surprisingly, the proposal for the e-commerce directive does not mention the DMCA, but is in certain parts almost verbatim.

The well-known triad in the e-commerce directive of the services provided by ISPs is mere conduit (Article 12), caching (Article 13), and hosting (Article 14). At first sight it may seem that the role of access providers is left unregulated. However, just as the DMCA covered access under 'transitory communications', the mere conduit of Article 12 regulates not only "the transmission in a communication network" but also "the provision of access to a communication network." The proposal also clearly indicates the different scope depending on the provider's role:

'establishes a "mere conduit" exemption and limits service provider's liability for other "intermediary" activities.'[26]

In order to be not held liable the access provider should not (a) initiate the transmission (b) select the receiver of the transmission; and (c) select or modify the information contained in the transmission. For an access provider, this set of conditions is even easier to comply with than the just discussed sixth conditions of the DMCA/OCILLA.

[23] Proposal for a EUROPEAN PARLIAMENT AND COUNCIL DIRECTIVE on certain legal aspects of electronic commerce in the internal market, 18.11.1998, COM(1998) 586 final, p. 4.

[24] At that time already some case law existed on ISP liability. For instance, in the Netherlands a lower court ruled in a law suit with Scientology Church and the Dutch ISP XS4ALL already on March 12 1996 (for a translated version of the summons, see http://kspaink.home.xs4all.nl/cos/dag1eng.html) . The case law was one of the reasons why the European Union considered it necessary to regulate the exemptions to liability: "To eliminate the existing legal uncertainty and to bring coherence to the different approaches that are emerging at Member State level." The final ruling by the Dutch Supreme Court on 16 December 2005 (LJN: AT2056) in the above mentioned case Scientology vs. XS4ALL is one of the few cases where the freedom of speech prevailed over copyright law.

[25] V. McEvedy (2002), The DMCA and the Ecommerce Directive, *E.I.P.R.* 2002, 24(2), 65-73.

[26] Proposal for a EUROPEAN PARLIAMENT AND COUNCIL DIRECTIVE on certain legal aspects of electronic commerce in the internal market, 18.11.1998, COM(1998) 586 final, p. 4.

III. Court orders and other observations

The fact that mere transmission and providing access are headed under the same category can be considered an underestimation of the role of access providers, as was indicated above. However, one could also argue that now both the DMCA and the E-commerce directive take this approach, there must be a reason why these services should be judged similarly. If we proceed from this assumption, we could argue that intervention of access providers should be treated similarly as intervention by providers of servers that just pass IP packets through. It is hardly imaginable that such a provider that only transmits information over the internet would ever be called upon. So, if this provider is headed under the same category as the access provider and never asked to assist with the enforcement of norms, why would the access provider be?

An obvious difference between the two providers is that the access provider has a contractual relationship with the user, and the provider merely passing through IP packets has not. However, the court cases discussed in this paper concern blocking access to certain sites, so the contractual relation is not relevant in that respect. Another difference has to do with the internet infrastructure. If an access provider blocks access this can be effective[27] to their users, and for the other provider the effect is not guaranteed. Moreover, all users worldwide could be effected by the latter measure, whereas actions from the access providers only effects their users.

The safe harbors created for access providers by both the DMCA and the e-commerce directive are not absolute. The DMCA is different in that it has an explicit notice and take down (NTD) procedure,[28] and providers can be forced to reveal the identity of subscribers. The e-commerce directive has no explicit procedures. As a consequence, IPSs need to carefully weigh pros and cons after a complaint without the certainty of not being held liable by either the party complaining or the opposing party. For the present paper this is not directly relevant, since access providers are never confronted with NTD requests, at least not in their role as access provider. Identity requests ask difficult decisions from ISPs, and these requests go even beyond the classic roles of ISPs and include web 2.0 providers.[29] Also identity requests fall outside the scope of the present paper.

An importance difference between the two regulatory frameworks is the way court orders are regulated. Whereas the DMCA defines many conditions that have to be met before a

[27] As is well known, measures not necessarily are effective, since circumvention is often quite easy.
[28] Section 512(c)(3) of the DMCA.
[29] P. Balboni *et al.* (2008), Liability of Web 2.0 Service Providers – A Comparative Look, *Computer Law Review International* Issue 3, pp. 65-71.

court can order an access provider to block certain content,[30] the e-commerce directive sets no specific conditions[31] but generally states in Article 12(3):

"This Article shall not affect the possibility for a court (…) requiring the service provider to terminate or prevent an infringement."

This might explain why it is relatively easy to get a court order within the EU, and hard to get one in the US. It might also explain why the tendency exists that within the EU the entertainment industry goes to court, and in the US they focus the introduction of new legislation. Illustrative are the Dutch court cases concerning the Pirate Bay, that we discuss next.

C. Dutch case law or the Pirate Bay saga

In 2012 the Dutch anti-piracy organization BREIN, a foundation which aims to enforce intellectual property rights for, basically, the entertainment industry, obtained several court orders that forced ISPs to block access to the Pirate Bay. The Dutch Pirate Bay cases nicely illustrate the legal grounds underlying the blocking of access by ISPs. Therefore the main arguments used in the various cases, that started with court proceedings against the Pirate Bay in May 2009, are discussed.

I. BREIN vs. the Pirate Bay 2009-2010

The case against the Pirate Bay maintains a bit of a history and began before the judge handed down its verdict in the Netherlands. Early in 2009, charges were filed in Sweden against the people behind the Pirate Bay, followed up by a conviction of one year imprisonment for Fredrik Neij, Gottfrid Svartholm, Peter Sunde, and Carl Lundström on April 17, 2009.[32] The criminal conviction in 2009 lead to the court initiative by BREIN, that sued the Pirate Bay people in the summer of 2009 for copyright violation.

The summons was delivered at the address as recorded in the Swedish population register, but was returned. The defendants did not show up in court, but the judge allowed the proceedings to take place in absentia.[33] This is allowed in summary proceedings if the plaintiff has put sufficient effort in trying to reach the defendant. Interesting in this case, is that the effort consisted, amongst others, in sending the court order via e-mail, Twitter, and Facebook (the plaintiff was de-friended minutes after the court order was left on the Pirate Bay owned Facebook page). Decisive was the reaction of one of the defendants when the

[30] § 512 (j)(2): "The court, in considering the relevant criteria for injunctive relief under applicable law, shall consider—
(A) whether such an injunction, either alone or in combination with other such injunctions issued against the same service provider under this subsection, would significantly burden either the provider or the operation of the provider's system or network;
(B) the magnitude of the harm likely to be suffered by the copyright owner in the digital network environment if steps are not taken to prevent or restrain the infringement;
(C) whether implementation of such an injunction would be technically feasible and effective, and would not interfere with access to noninfringing material at other online locations; and
(D) whether other less burdensome and comparably effective means of preventing or restraining access to the infringing material are available.

[31] M. Peguera (2009), The DMCA Safe Harbors and Their European Counterparts: A Comparative Analysis of Some Common Problems. *Columbia Journal of Law & the Arts*, Vol. 32, p. 481-512.

[32] Subsequently, in February 2012, the Swedish Supreme Court decided not to grant leave on appeal, and the case is now taken to the European Court of Justice.

[33] Court of Amsterdam 30 July 2009, LJN BJ4298, www.rechtspraak.nl/ljn.asp?ljn=BJ4298.

press confronted him with the upcoming court case: “Having a court case in Amsterdam on July 21, does not ring a bell.”

In the verdict the court ordered on 30 July 2009 the Pirate Bay to:

1. Stop copyright infringements in the Netherlands;
2. Make websites thepiratebay.org, piratebay.se, etc. inaccessible to Dutch users.

The verdict is somewhat ambiguous. What is probably meant by ‘Dutch users’ and “copyright infringements in the Netherlands” is Dutch IP addresses. One could argue that if the mentioned websites are inaccessible in the Netherlands copyrights infringements are stopped as far as The Pirate Bay is involved, so the first order does not add anything. However, the reason for the first point might be that changing domain names will not work to undermine the second point. Clearly, if a proxy is used the second ban can be circumvented, and allows users to access the Pirate Bay and infringe copyrights.

After this verdict The Pirate Bay started summary proceedings against BREIN. They argued that due to the technical complexity this case is not suited for summary proceedings. The judge indicated that despite the complexity, balancing the opposing interests of The Pirate Bay and BREIN remains possible. The Pirate Bay did not violate copyrights, but the judge decided that the act of facilitating copyright infringements by others is illegal. The judge ordered on 22 October 2009:[34]

1. Pirate Bay should delete all torrents that refer to material that infringes on copyright material relevant to BREIN;
2. Block access of Dutch internet users on the various Pirate Bay websites to the torrents under 1.

The idea behind this change in court order was to allow references to material that does not infringe on copyrights of the parties BREIN represents. This is in favor of the freedom of speech as far as non infringing material is concerned. However, since the court orders the deletion of torrents, also people not using a Dutch IP address would no longer be able to access them. In this respect the order reaches further than the previous court order. Another problem with the verdict is how The Pirate Bay can establish whether a torrent infringes on copyright of the parties BREIN represents.

II. Intermezzo: International hosting providers

Pirate Bay did not follow the court order, so BREIN turned to the access providers. In previous court cases in other countries Pirate Bay hosting providers had been sued. First, the Swedish courts decided that it was not allowed to host the Pirate Bay. Pirate Bay was offline for a couple of days, but then re-appeared on German servers. The German judge also ordered to stop hosting the Pirate Bay. The race to the bottom stopped in Ukraine, which is hosting the Pirate Bay servers since then. Except that suing in Ukraine would not necessarily have the same results as in Sweden and Germany, it became clear that even

[34] Court of Amsterdam 22 October 2009, LJN BK1067, www.rechtspraak.nl/ljn.asp?ljn=BK1067.

winning in Ukraine would only mean that The Pirate Bay would seek yet another country to host their websites.

III. BREIN vs. the largest ISP, summary proceeding 2010

Based on the just discussed verdict BREIN asked Dutch providers to filter out Pirate Bay internet traffic. The providers did not grant this request. Therefore, BREIN decided to sue only, in what they called a test case, the ISP that facilitated most Pirate Bay traffic. This appeared to be Ziggo. On principle grounds XS4ALL joint Ziggo as a defendant in this case.[35]

The subtlety of the 2009 verdict (not providing access to infringing material) was replaced by BREIN and became mere access. In summary proceedings BREIN applied the Dutch implementation of Article 11 of Directive 2004/48/EC on the enforcement of intellectual property rights (see also Article 8(3) Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society):

"(…) rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe an intellectual property right (…)"

The third party are the subscribers of the ISP. The judge did not grant the request, since he argued that the injunction is only allowed in cases of direct infringement, and the order would apply to all users of the provider, not only those infringing copyrights after accessing The Pirate Bay. This ruling is a bit odd: people who do infringe are banned, and people who do not infringe did not go to the Pirate Bay anyway. The argument could be that those who do not use the Pirate Bay might want to go there for lawful activities as well. However, in practice most, if not all, Pirate Bay users go there to obtain copies of works violating copyright.

IV. BREIN vs. the largest ISP, proceedings on the merits 2010-2012

In the proceedings on the merits that BREIN started after they lost the summary proceedings, they basically claimed the same.[36] The judge followed the European Court of Justice (ECJ) ruling from 12 July 2011[37] (Oreal/eBay), and stated that Article 11 of Directive 2004/48/EC on the enforcement of intellectual property rights can also be used to prevent infringements. In a later case (Scarlet/Sabam) on 24 November 2011[38] the ECJ indicated that active monitoring for illegal content cannot be asked from access providers.

This latter decision is interesting, since the verdict in summary proceedings of the Dutch judge was precisely asking this from the providers XS4ALL and Ziggo. If this verdict would be translated to ISPs it would not be allowed according to the Scarlet/Sabam-case. However, since BREIN chose a different strategy in which it asked the mere banning of domain names

[35] Court of The Hague 19 July 2010, LJN BN1445, www.rechtspraak.nl/ljn.asp?ljn= BN1445.
[36] Court The Hague 11 January 2012, LJN BV0549, www.rechtspraak.nl/ljn.asp?ljn= BN1445.
[37] Judgment of the Court (Grand Chamber) of 12 July 2011. L'Oréal SA and Others v eBay International AG and Others. Case C-324/09.
[38] Judgment of the Court (Third Chamber) of 24 November 2011. Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM). Case C-70/10. The filtering asked for was far stretching, see under 40: "filtering system would require: first, that the ISP identify, within all of the electronic communications of all its customers, the files relating to peer-to-peer traffic; secondly, that it identify, within that traffic, the files containing works in respect of which holders of intellectual-property rights claim to hold rights; thirdly, that it determine which of those files are being shared unlawfully; and fourthly, that it block file sharing that it considers to be unlawful."

and IP addresses this EU court ruling could not be applied directly. This actually means that due to BREIN claiming too much (hence, also blocking legal internet traffic), they could circumvent the active monitoring prohibition. Blocking websites or IP addresses of the Pirate Bay is ordered from the ISPs.

On the subsidiarity question the judge in the summary proceedings indicated that at least suing some consumers, i.a. because they could then have the opportunity to defend their position, could be asked from BREIN. Now the judge indicated this was not necessary, and that after the lawsuits against the Pirate Bay and the hosting providers, the logical next step concerned access providers.

On the proportionality question, the judge indicated that given the amount of illegal opposed to legal content, the interests of the copyright holders outweigh the interests of the ordinary internet users. Still, the blocking of access to the complete website is less proportional than what was previously ordered by the court: not providing access to illegal material. Interestingly enough, downloading music and movies is allowed in the Netherlands, but uploading of infringing material is illegal. Most though not all users do both on a torrent site.

During the proceedings BREIN claimed that blocking had been effective in Denmark and Italy. Still, it is easy to circumvent the blocking, and the people who really want to use the Pirate Bay can do so. Interestingly enough, research carried out by the University of Amsterdam showed no difference in Pirate Bay internet traffic after the ban.[39]

The judge briefly addresses the question whether the current measure is necessary in a democratic society cf. Article 10 ECHR. He refers to the just discussed proportionality and subsidiarity considerations, in particular regarding the interests of the subscribers in relation to the copyright holders. One might claim that the necessity considerations should at least include how the entertainment industry operated during the last 15 years.[40] Another point that could have been covered is what role access providers should have on the internet. The outcome might still have been the same, but it would have been better grounded.

The judge ordered Ziggo and XS4ALL to block a list of 24 websites (of which several where outdated at the moment of the verdict, and others later became outdated), as well as three IP addresses. Curious is that BREIN has the right to change the list anytime they believe this is necessary, without judiciary intervention. One could argue that the judge did not really take notice of the particular sites anyway, but in a trial opponents have the opportunity to object. Ziggo and XS4ALL now have to start a new trial if they do not agree with a particular IP address or website. If they do not comply they have to pay a daily fine. The verdicts does not pay attention to possible errs on the site of BREIN.

Both Ziggo and XS4ALL appealed, but a decision is not expected before the end of 2013.

[39] A report in Dutch by the System and Network Engineering research group is available at http://bit.ly/S9xcCZ, J. van der Ham *et al.* (2012), Review en Herhaling BREIN Steekproeven 7-9 april 2012

[40] See e.g., D.Y. Choi & A. Perez (2007), Online Piracy and the Emergence of New Business Models, *Technovation*, Volume: 27 Issue: 4 pp. 168-178.

V. BREIN vs. other ISPs 2012/5-

Based on the verdict BREIN asked other ISPs to voluntarily start blocking The Pirate Bay. Since the ISPs refused, BREIN started new proceedings against other big providers, viz. KPN, UPC, T-Mobile, and Tele2.[41] The verdict is lengthy, but does not add much. A difference with the original verdict is that BREIN is not allowed to change the list of sites and IP addresses. The Pirate Bay has over 100 different IP addresses and already announced that they might add one IP address at the time, meaning that BREIN will have to start over a hundred different procedures. Maybe, this Pirate Bay policy can change subsequent verdicts on this point.

One interesting observation is on the effectiveness of the blocking. The ISPs introduced the previously mentioned research by University of Amsterdam[42] that showed that the blocking did not have any effect. The judge states:

"blocking as such does not necessarily lead to less Pirate Bay traffic, but effectively combating infringements is possible only if this blocking is combined with other measures."

A somewhat curious observation, in particular since one of BREIN's claims has been from the beginning that the blocking has at least some effect and as such contributes to fighting copyright infringements. So, the argument is that the measures are a necessary element that work in combination with other measures. One of those other measures is to forbid proxy servers. In the course of 2012 BREIN sued a series of organizations and people that offered proxy servers, and did so ex parte.[43] One of the controversial cases was against the political Pirate Party. Although legally interesting and societal relevant, these cases are not within the scope of the present paper, since it does not concern access providers.

D. What role fits access providers best?

The decisions discussed above are certainly not exclusive to the Netherlands. On May 1, 2012, the High Court in the United Kingdom ruled that the major ISPs in the UK must block access to the Pirate Bay. As the providers themselves noted, they do not want to be the judge and the jury of online content. Copyright infringing material is the prime example of content ISPs are asked to intervene with and central in this paper.

The interest in ISPs commenced before the DMCA and Directive on e-commerce were enacted. Back in 1995 ISPs were considered to be the most suited party to control the dangers of the internet, "a task force created by President Clinton suggested imposing strict liability on ISPs."[44] Moore & Clayton capture the complexity of ISP liability,[45]but recognize how " (…) ISPs are in an unrivalled position to suppress content held on their systems."[46]

[41] Court The Hague 17 April 2012, LJN BW3596, www.rechtspraak.nl/ljn.asp?ljn= BW3596.
[42] See note 39.
[43] For a discussion of the Dutch ex parte practice, see *Ex parte decision against The Pirate Bay proxy causes controversy* on Future of Copyright: http://bit.ly/UgmcVj
[44] Mann & Belzey 2005, see note 18.
[45] T. Moore & R. Clayton (2008), The Impact of Incentives on Notice and Take-down. *Workshop on the Economics of Information Security* (WEIS).
[46] Ibidem.

Before answering the question what role the access provider fits best, we discuss ISP liability both related to internet traffic (spam, cyber security) and concerning content (defamation, privacy breaches, child porn). [47] For each of the topics we introduce a rule of thumb that can help ISPs in their decision to comply with a request or not.

I. Cyber security and spam: ISPs take initiative

In the field of cyber security ISPs have realized over the years that it is in their best interest to act. The same is true for spam. If ISPs would not use spam filters, probably no one would any longer use e-mail. Can ISPs still claim to be neutral if they actively act, such as in the case of filtering spam or eliminating malware?

In a famous Dutch case the Supreme Court judged on the position of an ISP in case of spam.[48] XS4ALL asked the direct marketer Ab.Fab to stop sending spam to their customers. Ab.fab did not. Some argued that ISPs would lose their neutral position should they be allowed to reject messages. The Supreme Court decided that an ISP had the right to ask stop sending spam.[49] The argument basically was that a provider is the owner of the mail server and if he does not want to process specific mails with good reason, he does not have to. Ab.fab was ordered to stop sending e-mail. Ironically, before the Supreme Court had ruled, Ab.fab already went bankrupt. The principle question still stood, whether the nature of the internet and the role of ISPs in it does not conflict with asking a company to not send unsolicited email. As with all rules or principles, exceptions apply. To draw a parallel, if a football stadium is open to the general public, some people causing trouble might be banned from the stadium. After such a measure the stadium is still open to the general public. So, in case of ISPs, certain traffic can be banned from their servers without ISPs' losing their neutrality. A similar argument applies to malware and other security measures.

In 2004 Lichtman and Posner called for an increased liability, and claimed that since ISPs are largely immune from liability they have no incentive to act.[50] Harper attacked this proposal pointing at a fundamental flaw:

"it places efficiency ahead of justice. The Internet is a medium, not a thing, and the supply of access to it is peculiarly unsuited to a liability rule like Lichtman proposes."[51]

Nonetheless, the position of Lichtman and Posner has been supported by, e.g., the United Kingdom House of Lords Science and Technology Committee, which stated in 2007 how

" (…) although ISPs could easily disconnect infected machines from their networks, there is no incentive for them to do so."[52]

[47] G. Sutter (2003): 'Don't Shoot the Messenger?' The UK and Online Intermediary Liability, *International Review of Law, Computers & Technology*, 17:1, 73-84

[48] Dutch Supreme Court 12 March 2004, LJN AN8483 (XS4ALL v. Ab.Fab).

[49] At that time the EU Directive 2002/58 on electronic communications had been enacted, and included an Article that banned spam in the EU, at least spam sent to natural persons.

[50] D.G. Lichtman & E.A. Posner, Holding Internet Service Providers Accountable (July 2004). *U Chicago Law & Economics*, Olin Working Paper No. 217, http://ssrn.com/abstract=573502.

[51] J. Harper (2005), Against ISP Liability. *Regulation*, Vol. 28, No. 1, pp. 30-33, Spring 2005.

[52] House of Lords: Science and Technology Committee (2007) *Personal internet security*: 5th report of session, Vol. 1: Report: 30.

Others echo similar notions. Chandler writes:

"[t]he parties best placed to address cyber insecurity, including (…) ISPs (…) do not face the full consequences of their contributions to cyber insecurity. Accordingly, they do not invest time and money to the socially optimal level of improved security".[53]

Van Eeten & Bauer challenge this assumption: ISPs may "(…) unwittingly reinforce the impression that they have few if any incentives to improve the security of their services".[54] This occurs through the resistance of ISPs to government intervention and the hesitance to surrender self-regulation. The resistance to government intervention is interpreted by many as an unwillingness to provide more security; yet, this is an incorrect conclusion according to Van Eeten & Bauer. The efforts made by ISPs to improve the security of their clients started to escalate during the last decade when ISPs began to understand how improved security turned out to be in their best interest. This is due to costs associated with insecurity of their clients.

As follows from the above discussion on spam and cyber security ISPs do take initiatives that in itself go beyond a neutral role of mere transport because it influences their core activities. Both spam and malware directly badly influence the (access) services. Their aim is to guarantee a good functioning internet, in particular access that is not hindered by unwanted (spam) and undesired (malware) activities of others. This is what justifies their action. The more related to their core activities actions by ISPs are, the less influence such actions have regarding their neutral position. In the end it should be the decision of the ISP, and not one imposed by, e.g., government. Because the ISP decides, and what they do is objectively good for their users, they can uphold their basic neutral position.

II. Requests related to content: child porn, defamation and right to be forgotten

If ISPs have no incentive external pressure could work. Access providers are in a position to influence what is communicated over the internet.

One should be very cautious in asking assistance from ISPs. The fact that it is technically possible, does not make it legally desirable. Assume there is a public meeting room in a building that is hired by a politically motivated group of people. During this meeting a defamatory poster is put on the wall. Assume some of the attendees inform the person who is defamed by the poster. He directly goes to the meeting and asks the people in the room to remove the poster. They do not. Could you imagine that the defamed person goes to the owner of the room to ask to remove the poster? In case you can imagine, do you believe he would do so or could be held liable if he did not? This is a very difficult decision for the third party to make. He has to balance the freedom of expression against the possible defamatory nature. Whilst this situation is already difficult to decide upon, what about the owner of the meeting room being asked to block access to the room because of the poster? This is even more difficult to decide upon, for the impact is bigger. If entrance to the room is blocked the people cannot have their meeting. This shows the indirectness of access blocking. The first

[53] J.A. Chandler. Liability for Botnet Attacks. *Canadian Journal of Law and Technology* (2006), Vol. 5: 1.
[54] M.J.G.van Eeten, & J. M. Bauer. Economics of Malware: Security Decisions, Incentives and Externalities. STI Working Paper 2008/1: 26.

level is asking the person who put the content there to remove it, the second level is asking the same to the hosting ISP, and the access providers only enters at the third level. In case judges order to block access to a particular website or IP-address this is because of the indirectness only acceptable as a last resort. But also then, a judge should be hesitant. For instance, because due to the nature of the internet such measures are both under and over inclusive.

Requests placed upon ISPs are often impractical and sometimes even illegitimate. The study carried out by Stol *et al.* on child pornography and internet filtering illustrates the difficult position of ISPs and the importance of solid legal analysis.[55] As Stol *et al.* conclude,

"[f]rom the point of view of constitutional law it is not acceptable that the authorities make use of instruments without sound legal basis in order to reach an otherwise legitimate goal. If the legislature's intention is to designate the blocking of child pornography as a duty of the police, then this should be provided in specific legal jurisdiction".[56]

It has been argued by Dommering[57] that a sound legal is impossible. The Dutch Constitution does not permit control in advance (censorship), and this filtering prevents the assessing of particular content. A rebuttal here is that the filtering takes place only on the basis of lists of websites and IP addresses where already child porn was found, so in this respect the control is afterwards and not preventive. However, the internet changes very quickly, and lists become outdated fast. One can never be sure what exactly is filtered.

Privacy breaches are another content related topic often taking place on the internet. Also, the internet hosts various outdated personal information or information one simply does not want to be confronted with any longer. It is not always easy to get this information offline. In a recent proposal the European Union introduced the *Right to be forgotten*.[58] Again, ISPs are asked to co-operate, which is complicated since they find themselves in the midst of a conflict of interest between freedom of speech and the right to privacy.[59] The one who has put the information is the first to contact, with the hosting provider coming second. One could imagine that access providers are asked to block certain content if these first two steps do not work.

[55] Stol, W.PH., Kaspersen, H.W.K., Kerstens, J., Leukfeldt, E.R. & Lodder, A.R. (2009). Governmental filtering of websites: The Dutch case. *Computer, Law & Security Review*, 25(3), 251-262.

[56] Ibidem. What happened in the Netherlands was that the police provided a list of sites to be blocked by ISPs. The ISPs only could see the sites that were on the list. In the research by Stol *et al*. it appeared that the was not updated regularly, contained websites that did not distribute child porn and of course missed many sites that did not. An additional problem with the initiative is that child pornography is hardly disseminated via public websites. The constitutional argument against this co-operation between police and ISPs was that the police asked ISPs to filter internet traffic, which is something the police would not be legally allowed to do. After the publication of the research the police stopped the co-operation with ISPs.

[57] E. Dommering (2008), Filteren is gewoon censuur en daarmee basta (filtering is always censoring), *Tijdschrift voor Internetrecht.*

[58] In Section 3 Rectification and Erasure, Article 17 (Right to be forgotten and to erasure) in COM(2012) 11 final, 25 January 2012, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

[59] G. Sartor (2012), *Providers' Liabilities in the New EU Data Protection Regulation: A Threat to Internet Freedoms?*, http://ssrn.com/abstract=2047428

III. Copyright infringement: external and preventive actions

A couple of years ago the discussion focused on the necessity of increased liability for ISPs, currently ISPs are just asked to carry out certain actions. The Dutch law suits by BREIN discussed above are a prime example, as is the French HADOPI act.[60] The background of HADOPI's "three strikes and you're out" introduced in 2009 is fighting copyright infringements. ISPs play a central role, e.g., after a first notice the ISP should actively monitor the suspect, and after the third "strike" the person in question is blacklisted. The provider of the violating user as well as other ISPs should ban the user for a fixed period of up to one year. This means that the access provider instead of blocking content, should cut off an individual from the internet. Besides this could conflict with human right s,[61] what is demanded from the access provider is the enforcement of norms that diametrically oppose their core activity: providing internet access to people.

Of a different nature is the initiative in 2011 where some of the biggest American providers did not need an Act or verdict, but voluntary agreed to become "copyright cops".[62] Probably these providers had reasons to act as such, but it puts their neutral role under pressure. For these providers it is difficult to claim that due to their neutral position they do not have to co-operate if asked by private parties or government to intervene, both repressive and preventive, in case of digital piracy.

There is an important distinction to be made here. On the one hand ISPs acting voluntarily, on the other hand ISPs being forced. Just as in case of child porn government should not force ISPs to block access, ISPs may do it on their own initiative. However, once you act freely, you can no longer claim to be neutral as far as similar content is concerned. Once ISPs are more than passively involved with, the communication or the flow of information, they cannot rely on the safe harbors created by law. This does not make them necessarily liable, but there is no longer an easy way out. The same is true for access providers: once you voluntary search for, e.g. copyright violations, thirds can ask you to do so too.

IV. Statutes and judges

We discussed Dutch cases that lead to various court orders forcing access providers to block the Pirate Bay. Different from what is currently happening within the EU, the US cannot count on the judiciary when it comes to blocking websites. The conditions as, e.g., formulated in the DMCA/OCILLA are simply too difficult to meet. That is one reason why the music industry tries to get Acts pushed through American Congress. Basically, getting a bill passed is more difficult than convincing a judge. Judges are not elected in the Netherlands (and in most, if not all, EU countries), so judges do not have to take public opinion into account. The US legal initiatives demonstrated that public opinion can influence the decision making process of parliament.

Recall that on January 18, 2012, over 7,000 websites, including Wikipedia and Google, successfully staged a blackout as a means to protest legislative initiatives introduced in both chambers of the United States Congress. These initiatives, the Stop Online Piracy Act (SOPA)

[60] http://www.hadopi.fr/ HADOP is also known as the *Creation and Internet Law* and stands for (freely translated) High Authority for the dissemination of works and the protection of rights on the Internet (in French: Haute Autorité pour la diffusion des oeuvres et la protection des droits sur Internet)

[61] Several countries acknowledge a fundamental, constitutional internet access right.

[62] http://news.cnet.com/8301-31001_3-20077492-261/top-isps-agree-to-become-copyright-cops/

as well as the Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act (PIPA), both aimed to curb digital piracy in the United States. The primary objectives of both bills was to promote prosperity, creativity, entrepreneurship, and innovation by combating the theft of U.S. property. Or, as the Economist put it more bluntly, "[t]he bill aims to cut off Americans' access to foreign pirate websites by squeezing intermediaries."[63]

Beside the general public's opportunity to influence, focus is another difference between legislation and court cases. In court cases the focus is on a single actor (e.g., Pirate Bay), which makes it easier to decide against him. Also related to focus is that proposals for legislation are necessarily abstract, and likewise feel more as a threat to the general public (e.g., it touches the whole internet). One additional difference we want to note is that politicians appear to feel more sympathy for the economic arguments of the entertainment industry than judges are expected to. Finally, public opinion can correct during the legislative process, whereas in court cases public opinion basically starts only after the decision: only then it becomes clear what the outcome is.

The position of access providers as a neutral is not different as it comes to objecting against case law or against acts. Only the means to maintain the neutrality are different.

V. How to draw the line?

The list of requests access providers receive is long, so we could not discuss all, e.g., data retention[64] or online porn blocking.[65] This expanding list, both in terms of what to do and how to do it, urges the need to reevaluate what is being asked from access providers.

Basically two camps exist. One camp stresses the importance of internet freedom, innovation, the neutral role of providers, protection of freedom of speech and privacy. The other camp stresses also innovation, protection of rights, fighting crime. And as with all discussions, there are intermediate positions. We take position in this debate, but emphasize that as with all legal debates and in particular concerning internet governance topics, there is no obvious right or wrong but about balancing, weighing pros and cons. In the fire of the discussion this is sometimes forgotten, but with sensitive issues important to keep in mind: arguments matter, not who is defending them.

In drawing the line between under what circumstances ISPs could be asked to cooperate, and when it is better to leave them, at least the following should be taken into account.

First, the *directness* of the measure. In a way this is related to but not the same as the question of subsidiarity: if other less burdensome actions are possible they should be preferred. Directness also concerns how related the proposed action is to the activities of the ISP. The more direct, the sooner action might be asked from ISPs. For instance, if someone wants to take material down the first to go to is the one who putted it there, next the hosting provider, and third the access provider.

[63] Rights and wronged: An American anti-piracy bill tries to stem the global theft of intellectual property http://www.economist.com/node/21540234

[64] F. Bignami (2007), Privacy and Law Enforcement in the European Union: The Data Retention Directive, 8 *Chicago Journal of International Law*, Spring 2007, p. 233-255.

[65] More than a third of Britons support online porn block, *Daily Telegraph, August 19 2012,* http://bit.ly/S84SiK

Second, the *effectiveness* of the measure. Each action serves a goal, but if the goal is hardly reached then someone might take action himself anyway but normally should not ask this from others. If a measure is mere symbolic, or the effects are insignificant, access providers should not be asked to cooperate. Basically, the more effect a measure has, the sooner action might be asked from ISPs. It might be that what is asked for is so important that even the slightest effect is worth carrying out the action. If that is the case, normally the action should be carried out unless the costs (not only financially) associated with the action are disproportional.

Third, the *costs* of the measure. This point is related to proportionality: the action should be in proportion to the severity of what is targeted at. The cost are, again, not only financially but may also concern effort or side effects. The lower the costs, the sooner action might be asked from ISPs. It may not become an argument in itself, or better, not the only argument. If an action scores bad on other aspects, and the only real argument is that it is easy for the access provider to fulfill the request, the ISP should not.

Fourth, *relevance* related to the history of the ISP. If an ISP has cooperated voluntary in the past in case of requests, or has taken actions himself related to what he is asked to do, it is harder to refuse assistance. The more related activities of the ISP in the past are to what he is asked to do, the sooner action might be asked.

Fifth, the *time* element. Repressive actions do not concern censorship, whereas preventive actions do.[66] If content is taken down, the action is clearly repressive and does concern only the content taken down. Blocking access to websites might even in case of repressive action turn into censorship. This has to do with the dynamic nature of the internet. In case of, e.g. cybercrime, assistance to block traffic to particular websites (cf. the black listing of servers sending spam) may also filter out legitimate e-mail. Therefore, any list of sites blocked should be evaluated regularly.

Finally, and this is an overreaching element, adequate *safeguards* should be in place. The points indicated above already imply warranties. In addition, for any action asked from ISPs there should be a sound legal ground. It is important to rule out arbitrariness. Also judiciary intervention can be part of the safeguards. At the wrong side of the border are, e.g., black box lists of websites so that ISPs do not know what they filter or lists of websites created without judicial intervention.

E. Concluding observations

In January 2012 a 10 year old Dutch boy (and obviously many others) could no longer download legal software via his favorite website. This was not because on January 11 the Court of The Hague ordered two providers to block the Pirate Bay, or because SOPA, PIPA or ACTA entered into force. It appeared that the US Department of Justice had taken the file-hosting site Megaupload offline. Ironically, or sadly, this was exactly the day after Wikipedia blacked out protesting against the SOPA and PIPA initiative.

[66] For an overview of internet filtering practices in Africa and Asia some years ago, see R. Deibert *et al.* (2008)(eds.), *Access denied*, The MIT Press, Cambridge, Massachusetts.

The Megaupload case is an interesting example of the strong, or better long, arm of the law. People (e.g., Kim Dotcom) were arrested by the FBI in amongst others New Zealand. The link between Megaupload and the US was not clear. Sure, the internet is accessible all over the world, information on a website enters basically all jurisdictions.[67] The reason, however, for US action was that the people behind Megaupload were accused of running an international criminal organization not only facilitating copyright infringements but also laundering money. This begs the question: why ask dozens, hundreds, or maybe even thousands of access providers to filter out websites, if one action against the provider of the website has the same result?

As the discussion of the Pirate Bay case revealed, it is not always easy to take a website offline. In case of the Pirate Bay successful court actions only led to shifting from hosting providers in one country to hosting providers in another country, lastly to the Ukraine.[68] So the call on access providers is comprehensible. Under circumstances they could be asked to assist. In this paper we introduced rules of thumb that could help in deciding whether an access provider should cooperate:

1. The more direct the requested action is, the sooner action might be asked from ISPs;
2. The more effect a measure has, the sooner action might be asked from ISPs;
3. The lower the costs, the sooner action might be asked from ISPs;
4. The more related activities of the ISP in the past are to what he is asked to do, the sooner action might be asked;
5. Repressive action is preferred over preventive, and preventive action needs regular re-evaluation;

Notably, adequate safeguards should be in place, in particular a sound legal basis for action. From the US perspective, Lemley, Levine & Post stated:[69]

"United States law has long allowed Internet intermediaries to focus on empowering communications by and among users, free from the need to monitor, supervise, or play any other gatekeeping or policing role with respect to those communications. Requiring Internet service providers (…) to block access to websites because of their content would constitute a dramatic retreat from that important policy."

We hope that the appeal cases in the Netherlands have other outcomes than the first instance decisions had. The US policy just described should be enforced (again) in the Netherlands as well as within other European Union countries. Access providers should not be forced to check lists of websites, IP addresses, and the like, for it concerns the opposite of what their role should be: providing access. An intermediary basically helps to connect

[67] Similar development is UK courts convicting people posting defamatory statements on Twitter, see e.g *Eurotech 28 March 2012* http://bit.ly/QEvqFN: "Now get this clear: someone from New Zealand feels insulted by a Indian official through a statement posted on Twitter which has its shiny new headquarters in San Francisco. Why would a British judge even accept this case?"

[68] Even a drastic action as in the Megaupload case would not have succeeded, since the US can shut down generic top level domains (.com, .org) but not top level country domains (piratebay.se).

[69] M. Lemley, D.S. Levine & D.G. Post Don't Break the Internet, December 19, 2011, 64 *Stan. L. Rev. Online* 34

two parties. We better not shut down train stations when the actual threat is somewhere down the line. Otherwise we are heading to a direction we should not want to go.[70]

[70] It could be the first slip of a slippery slope. See M Schellekens, "Liability of Internet Intermediaries: A Slippery Slope?", (2011) 8:2 *SCRIPTed* 154, who argued this is not the case.